Commercial Solutions for Classified: Transforming the IAD Delivery of IA Solutions

Commercial Solutions for Classified (CSfC) is the National Security Agency (NSA) business process for layering commercial technologies to protect classified information. It is founded on the principle that properly-configured, layered solutions can provide adequate protection of classified data in a variety of applications. NSA develops, approves, and publishes solution-level specifications called Capability Packages (CPs), and works with Technical Communities from across industry, governments, and academia to develop and publish product-level requirements in US Government Protection Profiles (PPs). The CSfC Program Management Office (PMO) serves as the focal point for executing the IAD commercial IA solution strategy, and partners with organizations across IAD and the NSA Commercial Solutions Center for expertise in engineering, analysis, risk assessment, testing, policy, and industry engagement.

Managing Risks Through Solution-level CPs

Recently, the CSfC PMO achieved several milestones after publishing the Data-At-Rest (DAR) and draft Mobile Access (MA) CPs. Both of these vendor-neutral specifications were written by the Trusted Engineering Group and are published on the CSfC public website on NSA.gov.

The first approved DAR CP meets the demand for data-at-rest solutions using NSA Suite B algorithms. The goal of the DAR CP is to protect classified data when the end user devices are powered off or unauthorized. Unauthorized, in this case, means prior to a user presenting and having its credentials (e.g., password, tokens, etc.) validated by both layers of a DAR solution.

The draft MA CP is intended to meet the demand for mobile solutions to protect classified data. Through the use of approved cryptographic algorithms, validated Common Criteria components, and layers of commercial products, the MA CP can meet customer requirements for domestic and international voice, video, and data capabilities from a mobile end user device. This CP, which was approved by the National Manager, Mr. Curt Dukes, in March 2015, describes the requirements to configure, test and monitor a layered solution using commercial technologies to access classified data remotely – with a smartphone or tablet. This solution-level design information, coupled with the product-level component listing on NSA.gov, helps National Security System (NSS) customers access the data they need, where and when they need it, to make better mission decisions.

Measures of Success

One of the key measures of the CSfC program's success is increasing the number of customers, operational systems, and requests for registered solutions. In each of these areas, the CSfC program is growing at an exponential rate.

Following separate IAD approvals, Secretary of Defense Communications, Department of Homeland Security and the White House Communications Agency, each, successfully registered voice-only mobile access initial solutions. These solutions are authorized to protect classified information using CSfC-

approved commercial products. As of 1 March 2015, there were 24 other customers who indicated intent to build solutions to comply with published CP requirements.

Another important measure of the CSfC program's success is increasing industry participation. The CSfC Components List on NSA.gov identifies commercial products satisfying reference architectures and configuration information in NSA CPs. Updates to this list are made frequently, highlighting how IAD is successfully moving at the speed of commercial technology.

The CSfC Components List initially debuted last year on NSA.gov with 33 components. Today, there are 227 components across 38 product lines from 10 different manufacturers covering the following technology areas: IPSec VPN Gateways, WLAN Access Systems, Certificate Authorities, IPSec VPN Clients, SIP Servers, Mobile Platforms, Mobile Device Management, Software Full Disk Encryption, VoIP Applications, and Traffic Filtering Firewalls. New components are added on an almost-weekly basis.

In order for a commercial product to be on the CSfC Components List, the vendor must have a signed Memorandum of Agreement (MOA) under the CSfC program, which stipulates compliance requirements with appropriate PPs and NIST FIPS 140-2, and compels the vendor to fix vulnerabilities in a timely manner. The Components List also has links to the selectable PP requirements that must be included in the Common Criteria evaluation of a product.

Trusted system integrators are instrumental to the success of the CSfC program because they build, test, document, and maintain CSfC solutions for customers. In addition, they often provide the necessary compliance information needed for decision makers responsible for approving the use of commercial IA solutions at their sites. To ensure there is a cadre of qualified trusted integrators, the CSfC program has a growing list of vetted commercial integrators published on NSA.gov. The first group of commercial integrators to satisfy the published criteria include: Army CERDEC, Assured Information Security, Booz Allen Hamilton, CDW-Government, General Dynamics C4 Systems, General Dynamics/Electric Boat Corporation, General Dynamics Information Technology, Key Management Solutions, L-3 Communications –East, Oceus Networks, and ViaSat.

CSfC PMO partners with other Information Assurance Directorate (IAD) organizations to draft and execute all the MOAs with vendors and integrators, and assist in keeping the CSfC website on NSA.gov and the NSA/PAO Twitter™ feed updated with recent CSfC information.

In The News

The CSfC program made its media debut recently on Fox News' cybersecurity show, "Firewall." In an engaging interview, the CSfC PM Andi Roddy described the CSfC program and how it is transforming the way IAD delivers IA solutions to its NSS customers. Not to be outdone, the print media weighed in with the publishing of a Network World article that highlighted how the CSfC program is improving security for everyone.

Looking Ahead

Since 2011, IAD has laid the foundation for CSfC by generating CPs and PPs, establishing the customer registration process, and by educating the stakeholder community. Today, as IAD continues to build on this firm foundation, the CSfC PMO is seeing the benefits of increased customer adoption of CSfC solutions and industry participation in the program. The focus of the CSfC PMO for 2015 will include the necessary operational emphasis on monitoring, incident reporting, and response – not just to support customers operationally, but to gather empirical evidence regarding the security performance of CSfC solutions. Additionally, a draft Committee on National Security Systems (CNSS) Advisory is being developed for external publication to provide the community an authoritative reference on CSfC. 2015 is shaping up to be a very productive year for the CSfC PMO.